

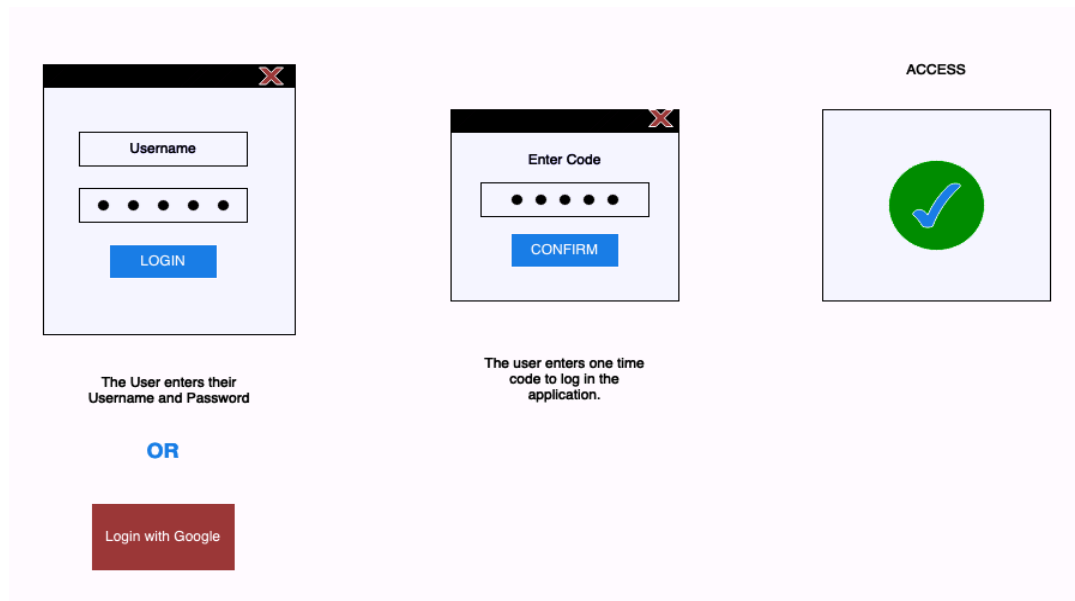
# Strong Authentication - MFA

## Introduction:

In the past when a user wanted to transfer money online, he had to log in to that bank's web application via his username and password. With impressive technological advancements, cyber crimes have increased as well. Hence, this username and password can be stolen by anyone. So in order to assure that the user who is attempting to log in using the username and password is actually the user, the bank's website uses Multi Factor Authentication(MFA). If this web site has been configured to perform MFA, the user who tries to log in to the web application has to give the username and password along with an additional authentication step, such as one-time password(OTP), sent to the user's mobile number. Hence, this transaction is safer than using only the username and password.




To demonstrate this scenario, we are going to log in to a sample web application called pickup-dispatch using MFA. In the first step the user has to provide their username/password. Once he is authenticated, the user receives a one-time password to their registered mobile phone.



## Setting up:

Create a Nexmo Service Provider application to configure OTP

1. Go to <https://dashboard.nexmo.com/sign-up> and sign up and start working with **SMS**.
  - a. This will create an API **key** and a **secret** for you.
2. Once the sign up is done, test it by clicking on **Send message**.



Nexmo is now Vonage

Balance  
€ 2.00 [upgrade](#)

2000 video test min

Account  
Master (d4cb1afb)

QUICKLINKS

- Billing
- Video Add-ons **new**
- Analytics
- Delivery and Quality
- Logs

MONITOR

- Fraud Defender **new**

BUILD & MANAGE

- API Settings
- Proactive Connect **new**

MG Account holder

## Try the SMS API

Try our API by sending an SMS to your phone. Sending SMS uses your account credit. [Learn more](#)

**Sending SMS in Sri Lanka**

Different countries have different standards and restrictions. Find out about SMS restrictions in Sri Lanka [here](#)

### Try it out

From  
Vonage APIs

Registered phone number  
[REDACTED]

This example only sends messages to the number you registered with

Message  
Hello from Vonage SMS API

**Send message**

**Your SMS has been accepted by our platform.**

You should soon receive it on your device if it is connected to the network. It will use €0.04

### Try it out with code


Use the provided code snippets to set up your own application.

cURL Node .Net Java PHP Python Ruby

**Write the code**

```
curl -X "POST" "https://rest.nexmo.com/sms/json" \
-d "From:Vonage APIs" \
-d "text:A text message sent using the Vonage SMS API" \
-d "to:[REDACTED]" \
-d "api_key=[REDACTED]" \
-d "api_secret=[REDACTED]"
```

- Goto the home screen using <https://dashboard.nexmo.com/> and the **API Key** and **Secret** are displayed in. Copy and save them as you need them for the next step.



Nexmo is now Vonage

Balance  
€ 0.04 [upgrade](#)

2000 video test min

Account  
Master (b9e0cc13)

QUICKLINKS

- Billing
- Video Add-ons **new**
- Analytics
- Delivery and Quality
- Logs

MONITOR

- Fraud Defender **new**

BUILD & MANAGE

- API Settings
- Proactive Connect **new**

AT asgardeo Account holder

Search for help

Welcome back, asgardeo

## Vonage API Dashboard

API key  
Master ([REDACTED])

API Secret  
[REDACTED]

**Platform status summary**

[Click here to view the full detail](#)

### Try our APIs

Discover how easy developing with our APIs can be 🧙

**Send an SMS**

Send and receive SMS from all over the world →

**Make a Voice call**

Build voice-based communication systems →

**Send a WhatsApp message**

Try our sandbox for Instagram, Viber, Facebook Messenger, and WhatsApp →

**Verify a user**

Two factor authentication made simple through an API →

**Look up a number**

Real-time intelligence on any phone number in the world →

**Create a video session**

Add interactive video and broadcasts to web and mobile apps, also in low-code. →

**More resources**

**SMS features and restrictions**

**You have € 0.04 free credit left**

Upgrading to a paid account will remove message watermarks, enable outbound traffic to any number, and allow the purchase of virtual numbers

[Add funds](#) →

**Set up account notifications**

Get alerts when your number subscriptions are due, your balance is low, or if our prices change

[Set up notifications](#)

**Add team members**

Our permission system makes collaboration easy

[Invite your team](#)

## Configure SMS OTP

1. Login to the WSO2 Identity Server **Console**, using your admin credentials (e.g. admin:admin).
2. In the WSO2 Identity Server **Console**, from the menu click **Connections**.
3. Open the **SMS OTP** local authenticator listed.
4. You will be prompted to the below page.

The screenshot displays the WSO2 Identity Server Console interface. On the left is a sidebar menu with options: Home, Applications, Connections (highlighted), API Resources, Branding, User Management, User Attributes & Stores, Organizations, Login & Registration, Email & SMS, Console Settings, and Server. The main content area is titled 'SMS OTP' with a subtitle 'Two-factor authentication using SMS one-time passcode.' Below the title are tabs for 'Quick Start' and 'Settings' (which is active). A blue notification bar states: 'Ensure that an SMS Provider is configured for the OTP feature to work properly.' The configuration form includes: 'SMS OTP expiry time' set to 5 minutes, with a note 'Please pick a value between 1 minute & 1440 minutes (1 day)'; a checked checkbox 'Use only numeric characters for OTP' with a note 'Please clear this checkbox to enable alphanumeric characters'; and 'SMS OTP length' set to 6 digits, with a note 'The number of allowed characters in the OTP. Please pick a value between 4-10.' An 'Update' button is at the bottom.

5. For the simplicity of this tutorial, let's keep the default configuration.
6. Create SMS Provider,
  - a. In the WSO2 Identity Server **Console**, from the menu click **Email & SMS**.
  - b. Select **SMS Provider**.
  - c. To create a Vonage SMS Provider click on the **Vonage** option.

- d. Paste the API **Key** and **Secret** you saved in [Create a Nexmo Service Provider](#) step.
- e. Enter the phone number you provided to Nexmo in the **Sender** field.

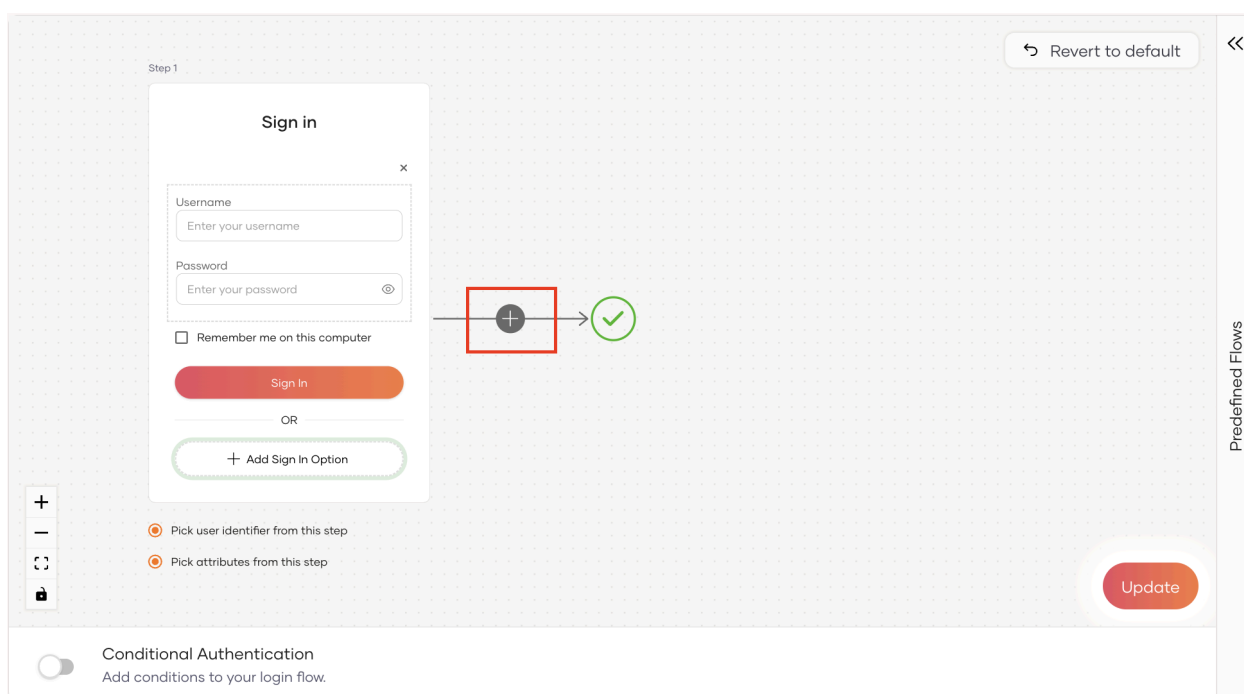
The screenshot shows the WSO2 Identity Server Console interface. On the left is a sidebar menu with options: Home, Applications, Connections, API Resources, Branding, User Management, User Attributes & Stores, Organizations, Login & Registration, Email & SMS (highlighted), Console Settings, and Server. The main content area is titled 'SMS Provider' with a subtitle 'Configure a SMS provider to send SMS to your users.' Below this are three tabs: Twilio, Vonage (selected and highlighted with an orange border), and Custom. The 'Vonage Settings' section contains three input fields: 'Vonage API Key' (with a red bar), 'Vonage API Secret' (with a red bar), and 'Sender' (with a red bar). Each field has a red asterisk indicating it is required. Below the 'Vonage API Key' field is a tooltip: 'Vonage API Key which act as username for the account.' Below the 'Vonage API Secret' field is a tooltip: 'The API Secret generated by the Vonage auth server.' Below the 'Sender' field is a tooltip: 'Phone number of the sender.' At the bottom of the form is a red 'Submit' button.

- f. Click **Submit**.

## Configure MFA to the sample application

Let's SMS OTP as the 2nd factor of authentication.

1. Use the **Dispatch** Application configured in **5. Single Sign-On with OpenID Connect Lab**.
2. In the WSO2 Identity Server **Console**, from the menu click **Applications**.
3. Click on application **Dispatch**.
4. Goto the **Login Flow**.
5. Click on **Revert to default**, to remove previously configured authentication mechanisms.
6. Next select **+** icon followed by the screen.



## 7. Click on the + Add Sign In Option of the 2nd step.

## 8. From the listed authentication methods, select **SMS OTP**.

9. Click **Update**.

## Update the user

1. In the WSO2 Identity Server **Console**, from the menu click **User Management**.
2. Select User.
3. From the list of users, select the user **Tommy**.
4. Add a **Mobile Number** to the respective fields.

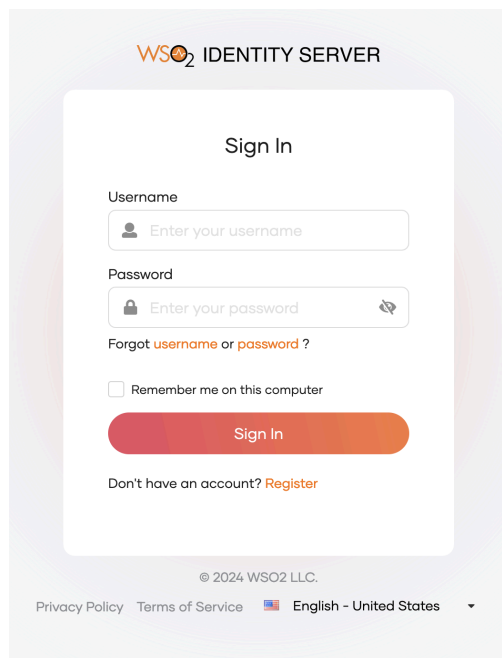
The screenshot displays the WSO2 Identity Server Console interface. On the left is a navigation menu with options: Home, Applications, Connections, API Resources, Branding, User Management (expanded), Groups, Roles, User Attributes & Stores, Organizations, Login & Registration, Email & SMS, Console Settings, and Server. The 'Users' option under 'User Management' is selected. The main content area shows the profile for a user named 'Tommy' (Tommy Kate). At the top, there is a 'Go back to Users' link and a user profile card. Below this, there are tabs for 'Profile', 'Groups', 'Roles', and 'Active Sessions'. The 'Profile' tab is active, showing a form with the following fields: User ID (fao0584d-dc44-44af-a490-96ffc1a0355d), Username (Tommy), First Name (Tommy), Last Name (Kate), Country (a dropdown menu showing 'Select your Country'), Email (asgardeo.test.user@gmail.com), and Mobile (94740877656).

5. Click **Update**.



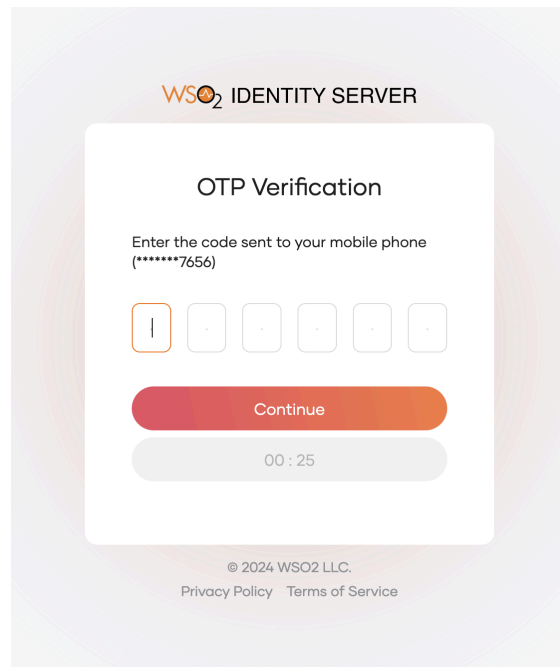
## Try It:

1. Go to <http://localhost.com:8080/pickup-dispatch> and click on the login button.
2. You will be redirected to the login page of WSO2 Identity Server. This login page consists of an option to enter the username and password. Type credentials of **Tommy**.



The screenshot shows the WSO2 Identity Server Sign In page. At the top, the WSO2 logo and 'IDENTITY SERVER' are displayed. The main heading is 'Sign In'. Below it, there are two input fields: 'Username' with a placeholder 'Enter your username' and a user icon, and 'Password' with a placeholder 'Enter your password', a lock icon, and an eye icon for toggling visibility. Below the password field is a link 'Forgot username or password?'. There is a checkbox labeled 'Remember me on this computer'. A large orange 'Sign In' button is centered below these options. At the bottom, there is a link 'Don't have an account? Register'. The footer contains the copyright notice '© 2024 WSO2 LLC.', links for 'Privacy Policy' and 'Terms of Service', and a language selector showing 'English - United States' with a dropdown arrow.

3. Once the above step is successful, you will be redirected to a page where you have to enter the one-time password(OTP) that has been sent to the mobile number configured in your profile.



WSO<sub>2</sub> IDENTITY SERVER

### OTP Verification

Enter the code sent to your mobile phone  
(\*\*\*\*\*7656)

1 . . . . .

Continue

00 : 25

© 2024 WSO2 LLC.  
[Privacy Policy](#) [Terms of Service](#)

4. Once you enter a valid OTP, you will be able to log in to the pickup-dispatch application. If you do not enter the OTP, you will not be able to log into the application due to an authentication failure.